mathematics

IMPACT FACTOR 2.2

CITESCORE 4.6

Article

# Application-Oriented Study of Next-Generation Alternant Codes over Gaussian Integers for Secure and Efficient Communication

Muhammad Sajjad and Nawaf A. Alqwaifly

Special Issue
Mathematics for Algebraic Coding Theory and Cryptography

Edited by
Dr. Mariana I. Durcheva

MDPI

https://doi.org/10.3390/math13142263

mathematics

MDPI

*Article*

# Application-Oriented Study of Next-Generation Alternant Codes over Gaussian Integers for Secure and Efficient Communication

**Muhammad Sajjad [1,*] and Nawaf A. Alqwaifly [2,*]**

[1] NUTECH School of Applied Science and Humanities, National University of Technology, Islamabad 44000, Pakistan
[2] Department of Electrical Engineering, College of Engineering, Qassim University, Buraydah 52571, Saudi Arabia
* Correspondence: muhammad.sajjad@nutech.edu.pk (M.S.); nkoiefly@qu.edu.sa (N.A.A.)

**Abstract**

This paper presents the construction and analysis of a novel class of alternant codes over Gaussian integers, aimed at enhancing error correction capabilities in high-reliability communication systems. These codes are constructed using parity-check matrices derived from finite commutative local rings with unity, specifically $\mathbb{Z}_n[i]$, where $i^2 = -1$. A detailed algebraic investigation of the polynomial $x^n - 1$ over these rings is conducted to facilitate the systematic construction of such codes. The proposed alternant codes extend the principles of classical BCH and Goppa codes to complex integer domains, enabling richer algebraic structures and greater error-correction potential. We evaluate the performance of these codes in terms of error correction capability, and redundancy. Numerical results show that the proposed codes outperform classical short-length codes in scenarios requiring moderate block lengths, such as those applicable in certain segments of 5G and IoT networks. Unlike conventional codes, these constructions allow enhanced structural flexibility that can be tuned for various application-specific parameters. While the potential relevance to quantum-safe communication is acknowledged, it is not the primary focus of this study. This work demonstrates how extending classical coding techniques into non-traditional algebraic domains opens up new directions for designing robust and efficient communication codes.

**Keywords:** alternant codes; Gaussian integers; finite commutative local rings; secure communication; wireless communications; digital storage; source codes

**MSC:** 94A24; 11T71; 11H71; 68P30



Academic Editors: Iliya Bouyukliev and Mariana I. Durcheva

Received: 25 May 2025
Revised: 17 June 2025
Accepted: 22 June 2025
Published: 13 July 2025

**Citation:** Sajjad, M.; Alqwaifly, N.A. Application-Oriented Study of Next-Generation Alternant Codes over Gaussian Integers for Secure and Efficient Communication. *Mathematics* **2025**, *13*, 2263. https://doi.org/10.3390/math13142263



## 1. Introduction

Algebraic coding theory is a cornerstone of modern information theory, enabling reliable transmission and storage of data over noisy channels. By introducing redundancy through structured mathematical codes, it allows for both the detection and correction of errors. One of the most versatile families of such codes is the class of alternant codes, which generalizes BCH and Goppa codes and combines algebraic flexibility with strong error correction capabilities. These codes are constructed using parity-check matrices derived from evaluations of rational functions, typically over finite fields.

Recently, research has explored the construction of alternant codes over more generalized algebraic structures, such as finite rings, Galois rings, and complex integer domains. One promising candidate in this direction is the ring of Gaussian integers, $\mathbb{Z}[i]$, which offers

additional algebraic tools such as norms, divisors, and Euclidean algorithms. Their structure enables more adaptable encoding mechanisms, particularly suitable for high-reliability systems such as satellite communication, the IoT, and 5G networks. Despite these prospects, the literature lacks a concrete coding framework for alternant codes over $\mathbb{Z}_n[i]$, where $n$ is a positive integer.

This paper addresses this gap by proposing a construction method for alternant codes over Gaussian integer residue rings, evaluating their structural properties, and analyzing their effectiveness in correcting errors across moderately sized block lengths.

### *1.1. Related Works*

The construction of error-correcting codes over non-field algebraic structures has received growing attention in recent decades. BCH and Goppa codes laid the foundation for alternant code construction. Huber extended this theory using Eisenstein–Jacobi integers, while Byrne and Fitzpatrick introduced alternant codes over Galois rings with efficient Hamming metric decoding. More recently, codes over Gaussian and Eisenstein integers have been explored for applications in both classical and quantum settings [1–7]. Sajjad et al. constructed BCH codes over Gaussian and Eisenstein fields and applied them in cryptographic systems [6,7]. Other works have linked alternant codes to Gröbner bases [8] and semigroup rings [9], while Shah and Medhat investigated the role of pullback constructions and integral domain properties [10–12]. Progress in quantum-safe cryptography has also intersected with this area. Xie et al. and Galindo et al. developed quantum error-correcting codes derived from classical BCH variants [13,14]. Lemoine et al. and Tang et al. enhanced decoding algorithms for alternant and GRS codes [15,16]. Different types of efficient codes and decoding strategies have been discussed in [17–19]. These studies collectively highlight the ongoing interest in applying algebraic structures beyond fields to construct robust, scalable codes.

### *1.2. Organization and Contributions*

The remainder of this paper is structured as follows:

- Section 2 outlines the algebraic preliminaries on Gaussian integers, residue class rings, and their impact on modern technology.
- Section 3 presents the construction of alternant codes over $\mathbb{Z}_n[i]$, with theoretical justifications.
- Section 4 includes decoding algorithms and performance evaluations.
- Section 5 includes a comparative analysis and discussion.
- Section 6 concludes the paper and outlines future research directions.

### *1.3. Major Contributions*

This work offers the following original contributions:

1. A New Algebraic Framework:

We develop a generalized framework for constructing alternant codes over residue class rings of Gaussian integers, $\mathbb{Z}_n[i]$, extending classical BCH principles.

2. Factorization of $x^n - 1$:

The factorization of $x^n - 1$ over $\mathbb{Z}_n[i]$ is analyzed to form the theoretical basis for parity-check matrix construction.

3. Efficient Encoding and Decoding Algorithms:

We provide procedures for encoding and syndrome-based decoding suited for Gaussian-integer based alternant codes, optimized for computational efficiency.

4. Performance Evaluation:

The proposed codes are evaluated in terms of redundancy, error correction capability, and complexity, particularly for medium-length codewords relevant to the IoT and segments of 5G.

5. Application Potential:

We demonstrate that the flexibility of $\mathbb{Z}_n[i]$-based codes opens opportunities for future use in quantum-safe and noise-resilient communication systems.

## 2. Gaussian Integers

By following Section 2 in [20], Gaussian integers (GI) ring $\mathbb{Z}[i] = \{b_0 + b_1 i : b_0, b_1 \in \mathbb{Z}\}$ is a subset of complex numbers, with multiplicative unit 1 and $i^2 = -1$. Let $g = a + bi$ be a Gaussian integer with conjugate $\overline{g} = a - bi$, and then the norm of Gaussian integer is $N(g)$ which is the product of a Gaussian integer with its norm (sum of squares of real part and coefficient of imaginary part) as $g\overline{g} = a^2 + b^2$. For example, $g = 2 + 3i$ is a Gaussian integer; its conjugate is $\overline{g} = 2 - 3i$. The norm of $g$ is $N(g) = (2 + 3i)(2 - 3i) = 2^2 + 3^2 = 13$. Multiplication of the norm of Gaussian integers satisfies the $N(g_1.g_2 \ldots g_n) = N(g_1).N(g_2) \ldots N(g_n)$, where $g_1, g_2, \ldots, g_n \in \mathbb{Z}[i]$.

**Theorem 1** ([21], Theorem 2.3.2.)**.** *The Gaussian ring* $\mathbb{Z}$[i] *is an integral domain.*

**Corollary 1** ([21], Corollary 2.4.2.1.)**.** *The integral domain* $\mathbb{Z}[i]$ *is an Euclidean domain.*

**Lemma 1** ([21], Lemma 3.1.1.)**.** *If* $\mathbb{Z}[i]$ *is a Euclidean domain, then* $\mathbb{Z}[i]$ *is a principal ideal domain.*

**Corollary 2** ([21], Corollary 6.2.4.1.)**.** *Let* $p \in \mathbb{Z}$ *be prime, with* $p \equiv 1 (\text{mod } 4)$*; then p can be factored into a product of the Gaussian prime in* $\mathbb{Z}[i]$*.*

**Corollary 3** ([21], Corollary 6.2.4.2.)**.** *Let* $p \in \mathbb{Z}$ *be prime, with* $p \equiv 1 (\text{mod } 4)$*; then p is not prime in* $\mathbb{Z}[i]$*.*

**Theorem 2** ([21], Theorem 6.2.5.)**.** *Let* $p \in \mathbb{Z}$ *be prime, with* $p \equiv 3 (\text{mod } 4)$*; then p is irreducible in* $\mathbb{Z}[i]$*.*

**Lemma 2** (Section 2 in [22])**.** *Let* $g = a + ib \in \mathbb{Z}_n[i]$ *is unit if and only if* $N(g)$ *is a unit in* $\mathbb{Z}_n$*.*

We observe that $\{\pm 1, \pm i\}$ are units in $\mathbb{Z}[i]$ and that Gaussian primes are the usual integers $p$ such that $p \equiv 3 (\text{mod } 4)$ and those Gaussian integers $\mathbb{Z}[i]$ such that $N(z) = p$. It can be seen easily that the ring $\mathbb{Z}[i]/n\mathbb{Z}[i]$ is canonically isomorphic to $\mathbb{Z}[i]_n = \{a + ib : a, b \in \mathbb{Z}_n\}$. This ring is denoted by $\mathbb{Z}[i]_n$, and it is a principal ideal ring, Definition 3.7. [22]; it suffices to fix $n \in \mathbb{Z}$ rather than fix $n$, such that $a + ib$. First, when $n$ is of the form $p^k$, where $p$ is a prime integer and $k > 0$. Since our main purpose is fields and local commutative rings of Gaussian integers, in this case, it may be noted that the ring $\mathbb{Z}_{p^k}[i]$ may not always be a local ring. Likewise, $\mathbb{Z}_p[i]$ is not a field for every prime $p$. We begin with the description of $\mathbb{Z}_{p^k}[i]$ for primes $p$ such that $\mathbb{Z}_{p^k}[i]$ is a local ring or field.

**Theorem 3** ([23])**.** *The ring* $\mathbb{Z}_{2^k}[i]$ *is local for every positive integer k.*

**Theorem 4** ([23])**.** *The ring* $\mathbb{Z}_{p^k}[i]$ *is local for every positive integer k and* $p \equiv 3 (\text{mod } 4)$*.*

**Corollary 4** ([6])**.** *Let* $\mathbb{Z}_{p^k}[i]$ *be a Gaussian field if* $p \equiv 3 (\text{mod } 4)$ *and* $k = 1$*.*

The following results characterize the unit elements of $\mathbb{Z}[i]_n = \mathbb{Z}_{p^k}[i]$. From Section 2 in [22];

(i) $U\left(\mathbb{Z}_{p^k}[i]\right) = 2^{2k-1}$, if $p \equiv 2$.

(ii) $U\left(\mathbb{Z}_{p^k}[i]\right) = \left(p^k - p^{k-1}\right)^2$, if $p \equiv 1(\text{mod } 4)$.

(iii) $U\left(\mathbb{Z}_{p^k}[i]\right) = p^{2k} - p^{2k-2}$, if $p \equiv 3(\text{mod } 4)$.

Impact of Alternant Codes in Modern Technology: Control and efficient data transfer in a constantly changing environment are crucial for the effectiveness of a number of exciting modern technological solutions, such as the 5G cellular network, computing in the cloud, automobiles without drivers, and the Internet of Things (IoT). These technologies depend on the high-speed accuracy of transmitting huge volumes of data in noisy and interfered areas. To overcome such issues, there is a need for the formulation of enhanced error-correction methods. This work proposes a new method in modern systems of communication by modeling the alternant codes built over the Gaussian integers. These codes are constructed based on parity-check matrices produced from finite commutative local rings created out of Gaussian integers modulo $n$. Thus, by integrating these alternant codes into data transfer processes, we advance the error detection and correction features of data transmission, thereby increasing its integrity and effectiveness. This study confirms that through the society of alternant codes, one can have strong support in responding to the challenges of modern communication systems; therefore, the given work can be regarded as significant progress in the sphere of coding and data transmission.

## 3. Alternant Codes

We explain the construction technique of alternant codes over the finite commutative local rings of Gaussian integers with identity. Initially, we list some data from the basic theory of commutative rings. Thus, $\mathbb{Z}[i]_n$ is assumed to be a finite local commutative ring with unity, $M$ is the maximal ideal of rings $\mathbb{Z}[i]_n$, and the residue field is $\mathrm{K} = \frac{\mathbb{Z}[i]_n}{M} \cong GF(q)$, where $q = p^m$ $m \in \mathbb{Z}^+$ and $p$ is a prime. Let $\mathbb{Z}[i]_n[x] = \left\{\sum a_j x^j : \forall a_j \in \mathbb{Z}[i]_n\right\}$. Let $g(x)$ be a monic polynomial of degree $s'$ in $\mathbb{Z}[i]_n[x]$, such that $\mu(g(x))$ is irreducible in $\mathrm{K}[x]$, where $\mu$ is a natural projection. Moreover, we would also conclude that $g(x)$ is irreducible because it gave a factorization of $h_j(x)$ in terms of lower-order cyclotomic polynomials and is irreducible in $\mathbb{Z}[i]_n[x]$. Suppose $R = \frac{\mathbb{Z}[i]_n[x]}{<g(x)>} \cong GR(p^k,\ s')$ is a finite commutative local ring with unity and is the Gaussian extension of $\mathbb{Z}[i]_n$ of degree $s'$. Its residue field will be $K_1 = \frac{R}{M_1} \cong GF\left(p^{ms'}\right)$, where $\overline{\mathrm{M}_1}$ is the maximal ideal of $R$. Let ${K_1}^*$ be the unit element $K_1$, and its order is $p^{ms'} - 1$. Suppose $R^*$ is the multiplicative group of $R$; then, as is customary with all multiplicative groups, it must be a direct product of cyclic groups. The cyclic group is the maximal cyclic subgroup of the group of units in $R$. The elements of that maximal cyclic group $G_s$ are the roots of the polynomial $x^s - 1$ for some $s$, where $gcd(s,\ p) = 1$, it is isomorphic to $K_1^*$. The cyclic group that is maximal then is denoted $G_s$ and has the order $s = p^{ms'} - 1$.

It has long been known that a parity=check matrix $H$ with $r$ rows and $n$ columns of elements from $G_s$ of $GF(q^m)$ can uniquely characterize an $(n,\ k_0)$ linear code over $GF(q)$, where $m,\ r \in \mathbb{Z}^+$ and $rm \geq n - k_0$.

**Definition 1.** *Given maximal cyclic subgroup $G_s$ of $\mathbb{Z}_{p^k}[i]^m$, assume that the locator polynomial $\eta = (\alpha_1,\ \alpha_2,\ \ldots,\ \alpha_n)$ consists of distinct elements of $G_s$ and $y = (y_1,\ y_2, \ldots,\ y_n)$ is an arbitrary vector consisting of the elements of $G_s$. Then, a parity-check matrix $H$ of shortened alternant code $C(n,\ \eta,\ y)$ of length $n \leq s$ over $\mathbb{Z}_{p^k}[i]$ is defined as follows:*

$$H = \begin{pmatrix} y_1 & y_2 & \dots & y_n \\ y_1\alpha_1 & y_2\alpha_2 & \dots & y_2\alpha_n \\ & & \ddots & \\ y_1{\alpha_1}^{r-1} & y_2{\alpha_2}^{r-1} & \dots & y_n{\alpha_n}^{r-1} \end{pmatrix},$$

*where* $r \in \mathbb{Z}^+$ *and* $r = n - k_0$. *Additionally,* $C(n,\ \eta,\ y)$ *is a linear alternant code* $[n,\ k_0,\ d]$ *over* $K = GF(p^m)$, *with* $n - mr \leq k_0 \leq n - r$. *The number of parity-check symbols is at most* $mr$. *Apart from it, it is possible to estimate the minimum Hamming distance for* $C(n,\ \eta,\ y)$ *from the parity-check matrix.*

**Theorem 6.** *It can also be seen that the minimum Hamming distance of alternant code* $C(n, \eta, y)$ *will be at least* $d \geq r + 1$.

**Proof.** Let $\mathrm{C(n, \eta, y)}$ be an alternant code of length n, where $\eta = (\eta_1, \dots, \eta_n) \in \mathrm{F_{q^m}}$ is a vector of distinct elements, $\mathrm{y} = (\mathrm{y_1}, \dots, \mathrm{y_n}) \in \mathrm{F_{q^m}}$ is a non-zero vector, and r is the designed error-correcting capability, i.e., the alternant code is derived from a Generalized Reed–Solomon (GRS) code of dimension $n - r$. The parity-check matrix $H$ of the alternant code is given by the following:

$$H = \left[\frac{1}{y_j}\eta_j^{i-1}\right]_{1 \leq i \leq r,\ 1 \leq j \leq n}.$$

□

Now, consider the minimum Hamming distance $d$. With the Singleton bound, for a code of length $n$, dimension $k$, and minimum distance $d$, we have $d \leq n - k + 1$. For an alternant code of length $n$, dimension $k \geq n - r$, since it is a subfield subcode of a GRS code over $F_{q^m}$. However, a key result from the theory of alternant codes tells us $d \geq r + 1$.

**Justification.** This is because any codeword $c = (c_1, \dots, c_n) \in C(n, \eta, y) \subset F_{q^n}$ satisfies: $Hc^T = 0$. Suppose $c$ has Hamming weight $w \leq r$. Then, the set of positions $j$ such that $c_j \neq 0$ has size $\leq r$. The submatrix of $H$ corresponding to those positions is a $r \times w$ Vandermonde-like matrix over $F_{q^m}$, and when $w \leq r$, such a matrix has linearly independent columns, unless $c_j = 0$ for all $j$, contradicting the assumption that $c$ has weight $w$. Hence, no non-zero codeword can have weight $\leq r$, implying $d \geq r + 1$.

**Example 1.** *For the impact of alternant codes constructed over Gaussian integers, let* $\mathrm{p} = 2$ *and* $\mathrm{k} = 1$, *then* $\mathbb{Z}_2[\mathrm{i}] = \{0,\ 1,\ \mathrm{i},\ 1 + \mathrm{i}\}$ *with* $\mathrm{i}^2 = -1$ *being the finite commutative local ring with identity having maximal ideal* $\mathrm{M} = \{0,\ 1 + \mathrm{i}\}$, *then the residue field* $\mathrm{K} = \frac{\mathbb{Z}_2[\mathrm{i}]}{\mathcal{M}} = \{\overline{0}, \overline{1}\} \cong \mathrm{GF}(2)$. *If* $\mathrm{g(x)} = \mathrm{x}^2 + \mathrm{x} + \mathrm{i}$, *then* $\mu(\mathrm{x}^2 + \mathrm{x} + \mathrm{i}) = \mathrm{x}^2 + \mathrm{x} + 1$ *it has no rational root and so it is irreducible over* K, *and* $\mathrm{g(x)} = \mathrm{x}^2 + \mathrm{x} + \mathrm{i}$ *is the basic irreducible over* $\mathbb{Z}_2[\mathrm{i}]$. *The given extension ring* $\mathrm{R} = \mathbb{Z}_2[\mathrm{i}][\mathrm{x}]/ < \mathrm{x}^2 + \mathrm{x} + \mathrm{i} > \cong \mathrm{GR}(2^4)$ *is the finite commutative local ring with residue field* $\mathrm{K_1} \cong \mathrm{GF}(2^2)$. *Then, the maximal cyclic subgroup* $\mathrm{G_s}$ *has the order* $\mathrm{s} = 3$. *For the purpose of generating the maximal cyclic group* $\mathcal{G}_3$, *let* $\alpha$ *be the root of* $\mathrm{g(x)}$ *and be of order of 6 in set* $\mathrm{R}^*$. *So,* $\alpha^2 = \alpha + \mathrm{i}$ *is the primitive root of* $\mathcal{G}_3$. *If* $\beta = \alpha + \mathrm{i}$, *then elements of* $\mathcal{G}_3$ *are* $\beta = \alpha + \mathrm{i}, \beta^2 = \alpha + \mathrm{i} + 1, \beta^3 = 1$. *Each of the elements of* $\mathcal{G}_s$ *are all the roots of* $(x^3 - 1)$ *(modulo* 2*). Now we choose* $n = 3$, $r = 2$, $\eta = (1,\ \beta,\ \beta^2)$, *and* $y = (1,\ 1,\ 1)$, *then* $C(3,\ \eta,\ y)$ *is the shortened alternant code with the parity-check matrix* $H$

$$H = \begin{pmatrix} 1 & \beta & \beta^2 \\ 1 & \beta^2 & \beta \end{pmatrix} = \begin{pmatrix} 1 & \alpha + i & \alpha + (1+i) \\ 1 & \alpha + (1+i) & \alpha + i \end{pmatrix},$$

*with a minimum distance* $d \geq 3$. *The corresponding parity-check matrix* $H'$ *of entries from the residue field* $K \cong GF(2)$ *is*

$$H' = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ .. & .. & .. \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}.$$

It is an established fact that the order of every finite field is a power of some prime $p$. From Corollary 4, $\mathbb{Z}_{p^k}[i]$ is a field if and only if $p \equiv 3(\text{mod } 4)$ and $k = 1$. Furthermore, the order of every finite field of Gaussian integers $\mathbb{Z}_p[i]$ with $p \equiv 3(\text{mod } 4)$ will be $p^2$.

**Example 2.** *For the alternant codes construction over Gaussian integers, let* $p = 3$ *and* $k = 1$; *then* $\mathbb{Z}_3[i] = \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\}$ *is a Gaussian field with 9 elements, and it is isomorphic to* $\mathcal{GF}(3^2)$. *Let* $f(x) = x^2 + x + (2+i)$ *is a primitive irreducible polynomial over* $\mathbb{Z}_3[i]$. *Let* $\alpha$ *be the root of* $f(x)$; *then,* $\alpha$ *has order* 80 *in* $\mathbb{Z}_3[i]$. *The remaining elements of extension field* $\mathbb{Z}_3[i]^{*2}$ *are given in Table 1.*

Let $\eta = (\alpha, \alpha^3, \alpha^{19}, \alpha^{51}, \alpha^{54}, \alpha^{57}, \alpha^{70}, \alpha^{75}, \alpha^{79})$ and $y = (\alpha, \alpha^7, \alpha^{19}, \alpha^{25}, \alpha^{27}, \alpha^{47}, \alpha^{60}, \alpha^{63}, \alpha^{71})$ then for $r = 3$, $C(9, \eta, y)$ has parity-check matrix

$$\mathcal{H} = \begin{pmatrix} \alpha & \alpha^7 & \alpha^{19} & \alpha^{25} & \alpha^{27} & \alpha^{47} & \alpha^{60} & \alpha^{63} & \alpha^{71} \\ \alpha^2 & \alpha^{10} & \alpha^{38} & \alpha^{76} & \alpha & \alpha^{24} & \alpha^{50} & \alpha^{58} & \alpha^{70} \\ \alpha^3 & \alpha^{13} & \alpha^{57} & \alpha^{47} & \alpha^{55} & \alpha & \alpha^{40} & \alpha^{53} & \alpha^{69} \end{pmatrix}.$$

The parity-check matrix $H'$ of elements from $\mathbb{Z}_3[i] \cong GF(3^2)$ is

$$H' = \begin{pmatrix} 0+0i & 2+0i & 1+2i & 1+2i & 0+2i & 1+0i & 0+2i & 1+1i & 0+0i \\ 1+0i & 1+2i & 1+2i & 2+1i & 1+1i & 2+1i & 0+0i & 2+1i & 1+1i \\ .. & .. & .. & .. & .. & .. & .. & .. & .. \\ 1+2i & 2+1i & 1+2i & 2+2i & 0+0i & 0+1i & 1+2i & 1+1i & 1+1i \\ 2+0i & 0+0i & 0+1i & 1+2i & 1+0i & 1+0i & 0+0i & 2+0i & 0+0i \\ .. & .. & .. & .. & .. & .. & .. & .. & .. \\ 2+1i & 0+1i & 2+1i & 1+0i & 1+0i & 0+0i & 2+0i & 0+2i & 0+1i \\ 2+2i & 2+0i & 0+1i & 2+1i & 2+0i & 1+0i & 0+0i & 1+0i & 0+1i \end{pmatrix}.$$

We have an alternat code $C[9, 6]$ over $\mathbb{Z}_{3^2}[i]$ with minimum distance $d \geq 4$. Then all columns of $H'$ are linearly independent, and $C(9, \eta, y)$ has a minimum distance of 9.

**Example 3.** *For the alternant code construction over Gaussian integers, let* $p = 3$ *and* $k = 2$, *then* $\mathbb{Z}_{3^2}[i]$ *is a local commutative ring with maximal ideal* $M = \{0, 3, 6, 3i, 3+3i, 6i, 3+6i, 6+3i, 6+6i\}$. *Further* $K = \{0, 1, 2, i, 1+i, 2+i, 2i, 1+2i, 2+2i\} \cong GF(3^2)$. *The polynomial* $f(x) = x^2 + 7x + (8+i)$ *is irreducible over* $\mathbb{Z}_{3^2}[i]$. *Thus,* $\mathcal{R} = \frac{\mathbb{Z}_{3^2}[i][x]}{<f(x)>}$ *is a Galois extension of* $\mathbb{Z}_{3^2}[i]$. *Let* $\alpha$ *be the root of* $f(x)$, *then* $\alpha$ *has the order* 240 *in* $\mathcal{R}^*$. *Let* $\beta = \alpha^3$ *generate a cyclic group* $\mathcal{G}_s$ *of order* $s = 3^4 - 1 = 80$. *If we set* $\eta = (1, \beta, \ldots, \beta^{79})$, *and* $y = (1, 1, \cdots 1)$ *for* $n = 80$ *and* $r = 4$, *we have an alternat code* $C[80, 76]$ *over* $\mathbb{Z}_{3^2}[i]$ *with a minimum Hamming distance of at least 5.*

**Table 1.** Elements of the multiplicative cyclic group $\mathcal{GF}(3^4) \cong \mathbb{Z}_3[i]^{*}$ [2].

| $\alpha^j$ | Values | $\alpha^j$ | Values | $\alpha^j$ | Values | $\alpha^j$ | Values |
|---|---|---|---|---|---|---|---|
| 1 | $\alpha$ | 21 | $i\alpha$ | 41 | $2\alpha$ | 61 | $2i\alpha$ |
| 2 | $2\,\alpha + 1 + 2i$ | 22 | $2i\alpha + i + 1$ | 42 | $\alpha + 2 + i$ | 62 | $i\alpha + 2i + 2$ |
| 3 | $2\alpha + 2 + i + 2i\alpha$ | 23 | $\alpha + 2 + 2i + 2i\alpha$ | 43 | $\alpha + 1 + 2i + i\alpha$ | 63 | $2\alpha + 1 + i + i\alpha$ |
| 4 | $2i\alpha + 1$ | 24 | $\alpha + i$ | 44 | $i\alpha + 2$ | 64 | $2\alpha + 2i$ |
| 5 | $i\alpha + 2i + 2 + \alpha$ | 25 | $2\alpha + i\alpha + 1 + 2i$ | 45 | $2\alpha + 1 + i + 2i\alpha$ | 65 | $\alpha + 2 + i + 2i\alpha$ |
| 6 | $i\alpha + \alpha + 2$ | 26 | $2\alpha + i\alpha + 2i$ | 46 | $2\alpha + 1 + 2i\alpha$ | 66 | $\alpha + i + 2i\alpha$ |
| 7 | $2i\alpha + \alpha + 2$ | 27 | $\alpha + i\alpha + 2i$ | 47 | $2\alpha + 1 + i\alpha$ | 67 | $2\alpha + i + 2i\alpha$ |
| 8 | $i\alpha + \alpha + i$ | 28 | $2\alpha + i\alpha + 2$ | 48 | $2\alpha + 2i\alpha + 2i$ | 68 | $\alpha + 1 + 2i\alpha$ |
| 9 | $2\alpha + 2$ | 29 | $2i\alpha + 2i$ | 49 | $\alpha + 1$ | 69 | $i\alpha + i$ |
| 10 | $2 + i$ | 30 | $2i + 2$ | 50 | $1 + 2i$ | 70 | $1 + i$ |
| 11 | $2\alpha + i\alpha$ | 31 | $2i\alpha + 2\alpha$ | 51 | $\alpha + 2i\alpha$ | 71 | $\alpha + i\alpha$ |
| 12 | $\alpha + 2i + 2i\alpha$ | 32 | $\alpha + 1 + i\alpha$ | 52 | $2\alpha + i + i\alpha$ | 72 | $2\alpha + 2 + 2i\alpha$ |
| 13 | $2\alpha + i$ | 33 | $2i\alpha + 2$ | 53 | $\alpha + 2i$ | 73 | $i\alpha + 1$ |
| 14 | $\alpha + 2 + i + i\alpha$ | 34 | $2\alpha + 2 + 2i + i\alpha$ | 54 | $2\alpha + 1 + 2i + 2i\alpha$ | 74 | $\alpha + 1 + i + 2i\alpha$ |
| 15 | $\alpha + 2$ | 35 | $i\alpha + 2i$ | 55 | $2\alpha + 1$ | 75 | $2i\alpha + i$ |
| 16 | $\alpha + 1 + 2i$ | 36 | $i\alpha + i + 1$ | 56 | $2\alpha + 2 + i$ | 76 | $2i\alpha + 2i + 2$ |
| 17 | $2i\alpha + 1 + 2i$ | 37 | $\alpha + 1 + i$ | 57 | $i\alpha + i + 2$ | 77 | $2\alpha + 2 + 2i$ |
| 18 | $\alpha + 2 + 2i$ | 38 | $i\alpha + 1 + 2i$ | 58 | $2\alpha + i + 1$ | 78 | $2i\alpha + 2 + i$ |
| 19 | $\alpha + 2i\alpha + 1 + 2i$ | 39 | $\alpha + i + 1 + i\alpha$ | 59 | $2\alpha + 2 + i + i\alpha$ | 79 | $2\alpha + 2 + 2i + 2i\alpha$ |
| 20 | $i$ | 40 | 2 | 60 | $2i$ | 80 | 1 |

## 4. Decoding Procedure

In this section, our intention is to demonstrate how the Euclidean algorithm can be used to decode alternant codes. Given $C(n,\ \eta,\ y)$, an alternant code over $GF(q)$ with parity-check matrix $H$, let the code have minimum distance $d = r + 1$. Let $c = (c_1,\ c_2,\ \ldots,\ c_n)$ be the transmitted codeword and $a = (a_1,\ a_2,\ \ldots,\ a_n)$ be the received vector. The error vector is defined as $e = (e_1,\ e_2,\ \ldots,\ e_n)$. Let $t = \lfloor \frac{r}{2} \rfloor$ errors that have happened in sites to decode alternant codes

$$X_1 = \alpha_{i_1},\ X_2 = \alpha_{i_2},\ \ldots,\ X_t = \alpha_{i_t}$$

In $\mathcal{G}_s$ with error values

$$Y_1 = a_{i_1},\ Y_2 = a_{i_2},\ \ldots,\ Y_t = a_{i_t}$$

Firstly, find the syndromes using

$$S = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ y_1\alpha_1 & y_2\alpha_2 & \cdots & y_2\alpha_n \\ & & \ddots & \\ y_1{\alpha_1}^{r-1} & y_2{\alpha_2}^{r-1} & \cdots & y_n{\alpha_n}^{r-1} \end{pmatrix} \begin{pmatrix} 0 \\ 0 \\ . \\ Y_t \\ . \\ 0 \end{pmatrix} = \begin{pmatrix} s_0 \\ s_1 \\ . \\ . \\ . \\ s_{r-1} \end{pmatrix},$$

where

$$S_\mu = \sum_{v=1}^{t} \alpha_{i_v}^{\mu} a_{i_v} y_{i_v} = \sum_{v=1}^{t} X_v^{\mu} Y_v y_{i_v}, \text{ For } \mu = 0,\ 1, \ldots r-1.$$

Secondly, find error locator polynomial $\sigma(z)$ as

$$\sigma(z) = \prod_{i=1}^{t}(1 - X_i z) = \sum_{i=0}^{t} \sigma_i z^i,\ \sigma_0 = 1.$$

Using syndromes, and the error evaluator polynomials

$$\omega(z) = \sum_{v=1}^{t} Y_v w_{i_v} \prod_{\substack{\mu = 1 \\ \mu \neq v}}^{t} (1 - X_\mu z).$$

Furthermore,

$$\frac{\omega(z)}{\sigma(z)} = S(z) (\text{mod } (z^r)),\ \text{where } S(z) = \sum_{0}^{r-1} S_\mu z^\mu.$$

Using the Euclidean algorithm, the above equation can be solved by

$$r_{-1}(z) = z^r \text{ and } r_0(z) = S(z).$$

Let is continue this Euclidean algorithm until $r_k(z)$ such that $deg(r_{k-1}) \leq \frac{r}{2}$ and $deg(r_k) \geq \frac{r}{2} - 1$. Then, the error locator polynomial and error evaluator polynomial are $\sigma(z) = \delta U_k(z)$ and $\omega(z) = (-1)^k \delta r_k(z)$, where constant $= \delta$. Chosen to make $\sigma(0) = 1$ and $U_k$ satisfies $r_k(z) \equiv (-1)^k U_k(z) r_0(z)\ (\text{mod } (r_{-1}(z)))$, and then

$$\omega(z) \equiv (\sigma(z) S(z)) (\text{mod } (z^r)),\ deg(\sigma(z)) \leq \frac{1}{2} r,\ \text{and } deg(\omega(z)) \leq \frac{1}{2} r - 1.$$

Lastly, find the error magnitudes using

$$\overline{Y}_\mu = \frac{\omega\left(X_\mu^{-1}\right)}{y_{i_\mu} \prod_{v \neq \mu}^{t} \left(1 - X_v X_\mu^{-1}\right)}$$

The pseudo code of the decoding procedure is given in Algorithm 1.

**Algorithm 1: Decoding Alternant Codes Using Euclidean Algorithm**

**Input:**

- Alternant code C(n,η,y) over GF(q)
- Received vector a = (a_1, a_2, . . ., a_n)
- Parity-check matrix H
- Set of support elements α = (α_1, α_2, . . .,α_n)
- Set of multipliers y = (y_1, y_2, . . ., y_n)
- Minimum distance d = r + 1
- Error-correcting capability t = $\lfloor r/2 \rfloor$

**Algorithm 1:** *Cont.*

**Step 1: Syndrome Calculation**

1. Initialize syndromes S_0, S_1, . . ., S_{r − 1} to zero.
2. For μ = 0 to r − 1:
    - S_μ = ∑{j = 1}^{n} aj·α_j μ·y_j

**Step 2: Define Syndrome Polynomial**

- Construct the syndrome polynomial:
  S(z) = S_0 + S_1 z + S_2 z^2 + . . . + S_{r − 1} z^{r − 1}

**Step 3: Apply the Euclidean Algorithm**

1. Initialize:
    - r_{−1}(z) = z^r
    - r_0(z) = S(z)
    - U_{−1}(z) = 0
    - U_0(z) = 1
2. While deg(r_k(z)) > ⌊r/2⌋:
    - Perform polynomial division:
      q_k(z) = ⌊r_{k − 2}(z)/r_{k − 1}(z)⌋
    - Update:
        - r_k(z) = r_{k − 2}(z) − q_k(z).r_{k − 1}(z)
        - U_k(z) = U_{k − 2}(z) − q_k(z).U_{k − 1}(z)
3. Let:
    - σ(z) = δ·U_k(z), where δ is chosen such that σ(0)=1
    - ω(z) = (−1)^k·δ·r_k(z)

**Step 4: Find Error Locations**

1. Find the roots of σ(z) = 0, say X_1^{−1}, X_2^{−1}, . . ., X_t^{−1}
2. Error locations are at positions where α_i = X_j for some j

**Step 5: Compute Error Values**

For each error location X_μ, compute the error magnitude:

$$Y^{-}\mu = \omega(X\_\mu^{-1})/(y\_i\mu \cdot \prod v \neq \mu(1 - X\_v \cdot X\_\mu^{-1}))$$

**Step 6: Recover the Original Codeword**

1. Initialize error vector e = (0, 0, . . ., 0)
2. For each error location i_μ, set e_iμ = Y^{−}
3. Compute corrected codeword:
   c = a − e

End

**Example 4.** *From Illustration 3.1, the maximal cyclic subgroup* $\mathcal{G}_3$, $\eta = (\beta^2, 1, \beta) = (\eta_1, \eta_2, \eta_3)$, $y = (\beta, \beta, 1)$ *and* $r = 2$, *so* $t = 1$ *with length 3 of alternant code* $\mathcal{C}(\eta, y)$ *over* $\mathbb{Z}_2[i]$ *with a minimum Hamming distance of at least 3. Let*

$$H = \begin{pmatrix} \beta & \beta & 1 \\ \beta^3 & \beta & \beta \end{pmatrix},$$

*be the parity=check matrix. Consider a received vector* $r = (0, 0, \beta^2)$, *and* $S = r\mathcal{H}^T = (\beta^2, \beta^3)$ *are two syndromes corresponding to the received vector r, which is non-zero; this means that r is not a codeword. Secondly, find the error locator polynomial* $\sigma(z)$ *for the weight of the received vector r, which is 1. Let* $t = 1$, *because only one component in r is non-zero. So,* $r_{i_1} = r_3$, *for* $i_1 = 3$; *this means the error is occurring at the third place in r. The location of the error is* $X_1 = \eta_{i_1} = \beta$, *with error magnitude* $Y_1 = r_{i_1} = \beta^2$. *The error locator polynomial is* $\sigma(z) = 1 - \beta z = 1 + \beta z$. *Furthermore, the error evaluator polynomial is* $\omega(z) = S(z).\sigma(z) \ (mod\ z^2) = \beta^2$, *where* $S(z) = \beta^2 + \beta^3 z$. *Finally, the error magnitude is* $\overline{Y}_1 = \beta^2$. *Hence,* $c = r - e = (0, 0, 0)$ *is a corrected codeword of the alternant code over* $\mathbb{Z}_2[i]$.

**Example 5.** *From Illustration 3.2, the cyclic group of order 80. Let us set* $\eta = (\alpha^2, \alpha, \alpha^{55}, 0, 0, \ldots, 0)_{1\times 10} = (\eta_1, \eta_2, \eta_3, \ldots, \eta_{10})$, $y = (1, 1, 1, \ldots, 1)_{1\times 10}$ *and* $r = 4$, *so* $t = 2$ *then we have length 10, and the alternant code* $\mathcal{C}(\eta, y)$ *over* $\mathbb{Z}_3[i]$ *with minimum Hamming distance is at least* 5 . *Let*

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & \ldots & 1 \\ \alpha^2 & \alpha & \alpha^{55} & 0 & \ldots & 0 \\ \alpha^4 & \alpha^2 & \alpha^{30} & 0 & \ldots & 0 \\ \alpha^6 & \alpha^3 & \alpha^5 & 0 & \ldots & 0 \end{pmatrix},$$

*be the parity-check matrix. Let a received vector* $r = (1, \alpha^2, 0, \ldots, 0)_{1\times 10}$ *and* $S = a\mathcal{H}^T = \begin{pmatrix} 1+\alpha^2 \\ \alpha^2+\alpha^3 \\ \alpha^4+\alpha^4 \\ \alpha^6+\alpha^5 \end{pmatrix} = \begin{pmatrix} \alpha^{77} \\ \alpha^{51} \\ \alpha^{44} \\ \alpha^{54} \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{pmatrix}$ *are the four syndromes corresponding to the received vector r, which are non-zero; this means that r is not a codeword. Secondly, find the error locator polynomial* $\sigma(z)$. *Let* $t = 2$ *because there are two non-zero components in r. So,* $r_{i_1} = r_1$, *and* $r_{i_2} = r_2$, *for* $i_1 = 1$, *and* $i_2 = 2$; *this means the error occurs in the 1st and 2nd places in r. The error locations are* $X_1 = \eta_{i_1} = \eta_1 = \alpha^2$ *and* $X_2 = \eta_{i_2} = \eta_2 = \alpha$, *with error magnitudes* $Y_1 = a_{i_1} = 1$ *and* $Y_2 = a_{i_2} = \alpha^2$. *Let the error locator polynomial* $\sigma(z) = 1 + \alpha^{10}z + \alpha^3 z^2$, *and the error evaluator polynomial is* $\omega(z) = \alpha^{28}z + \alpha^{77}$. *Further polynomials* $\sigma(z)$ *and* $\omega(z)$ *satisfy* $\sigma(z) = \omega(z)S(z)$ *mod* $(z^4)$. *Finally, the error magnitudes are*

$$\overline{Y}_1 = \frac{\omega(X_1)}{Y_1\left(1-X_2X_1^{-1}\right)} = \frac{\omega\left(\alpha^{78}\right)}{1\left(1-X_2X_1^{-1}\right)} = \frac{2+\alpha+i+i\alpha}{2+\alpha+i+i\alpha} = 1.$$
$$\overline{Y}_2 = \frac{\omega(X_2)}{Y_1\left(1-X_1X_2^{-1}\right)} = \frac{\omega\left(\alpha^{79}\right)}{1\left(1-X_1X_2^{-1}\right)} = \frac{2+i\alpha+i}{1+2\alpha} = 1+2\alpha+2i = \alpha^2.$$

Therefore, the error pattern is $e = (1, \alpha^2, 0, 0)$ and the corrected codeword is $c = (0, 0, 0, 0)$.

## 5. Comparative Analysis and Discussion

This section provides a comparative study of alternant codes over Galois rings and Gaussian rings, referring to the concept from Norton and Sălăgean [4] and Byrne and Fitzpatrick [8]. Two-dimensional vector algebra for local rings and fields is divided into two cases: Gaussian and Eisenstein. Eisenstein is discussed in our previously published article [16] in 2025. We cannot compare the proposed work with Eisenstein integers [16], because both Gaussian and Eisenstein integers have different congruence classes dependent on parameters $p$ and $k$. As a type of error-correcting code, alternant codes are studied in terms of various parameters, including the code length $n$, dimension $k'$, minimum distance $d$, ability to detect errors $(d-1)$, ability to correct errors $\left(t = floor\left(\frac{d-1}{2}\right)\right)$, code rate $R = k'/n$ and the number of codewords $|C|$. A comparative study of alternant codes over Gaussian rings $\mathbb{Z}_{p^k}[i]^s$ and Galois rings $GR\left(p^k,\ s\right)$ is given in Table 2.

**Table 2.** Comparative analysis of alternant codes over Galois rings and Gaussian rings.

| Structure | Reference | $n$ | $k'$ | $d$ | $d-1$ | $t$ | $R$ | $\|C\|$ |
|---|---|---|---|---|---|---|---|---|
| $\mathbb{Z}_2[i]^2$ | Proposed | 3 | 1 | 3 | 2 | 1 | 0.3333 | 16 |
| $\mathbb{Z}_3[i]^2$ | Proposed | 9 | 6 | ≥4 | ≥3 | ≥1 | 0.6667 | $3^{24}$ |
| $\mathbb{Z}_{3^2}[i]^2$ | Proposed | 80 | 76 | ≥5 | ≥4 | ≥2 | 0.95 | $3^{304}$ |
| $GR(2^2,\ 2)$ | [11,22] | 3 | 1 | 3 | 2 | 1 | 0.3333 | 4 |
| $GR(3^2,\ 2)$ | [11,22] | 9 | 6 | ≥4 | ≥3 | ≥1 | 0.6667 | $3^{12}$ |
| $GR(3^2,\ 4)$ | [11,22] | 80 | 76 | ≥5 | ≥4 | ≥2 | 0.95 | $3^{152}$ |

Based on the tabulated results, we can see that alternant codes over Gaussian rings provide a much larger codebook size $|\ C\ |$ compared to their counterpart over Galois rings, with the same value of code parameters n, k, and d. For instance:

- When $n = 3,\ k' = 1,\ d = 3$, the minimum distance and the code rate $(R = 0.3333)$ are the same when using $\mathbb{Z}_2[i]^2$ and $GR(2^2,\ 2)$; however, the code over the Gaussian ring has four times as many codewords $(|C| = 16$ versus $|C| = 4)$.
- In the case of $n = 9,\ k' = 6,\ d \geq 4$, $\mathbb{Z}_3[i]^2$ and $GR(3^2,\ 2)$ have the same structural parameters and error correction ability, but the Gaussian ring construction has twice the number of codewords $(3^{24}$ vs. $3^{12})$.
- A greater advantage is seen in larger lengths like $n = 80,\ k' = 76$, where both $\mathbb{Z}_{3^2}[i]^2$ and $GR(3^2,\ 4)$ provide five or more minimum distances and approximately the same code rate $(R = 0.95)$ but the code over the Gaussian ring has exponential growth in the number of codewords, with $|C| = 3^{304}$, whereas the Galois ring has $|C| = 3^{152}$.

A direct consequence of this doubling of the codeword length in all examples is that this suggests a more abundant codebook and, consequently, greater redundancy and more error resilience with Gaussian rings. The algebraic view as a Gaussian integer, especially the complex units and extra symmetry, enables more valid codewords with the same constraints. There is, however, a trade-off with this benefit: a bigger codebook means increased complexity in decoding and possibly lower transmission speeds because of the symbol space. Nevertheless, where error tolerance and robustness are valued, as in deep-space communication, military systems, or quantum-safe protocols, it is very desirable to use alternant codes instead of Gaussian rings.

Finally, it can be seen that alternant codes over Gaussian rings not only inherit the crucial parameters of the classical alternant codes over Galois rings but also surpass them in the abundance of codewords, making them more useful in the settings where the error correction capabilities are given the highest priority. These results confirm the potential of Gaussian rings as an algebraic basis to realize superior and powerful coding schemes.

## 6. Conclusions and Future Directions

In this article, the construction and analysis of alternant codes over Gaussian integers have been introduced with respect to their algebraic background and relevance in dependable digital communication. Using parity-check matrices whose entries are elements of finite commutative local rings with unity, namely, quotient rings of Gaussian integers modulo $n$, we have created a unified framework to construct error-correcting codes and generalize the classical BCH codes' paradigms. We have shown that these codes share structurally desirable properties with the Gaussian integer ring, including a more intricate algebraic structure and the existence of unit elements, which can help to achieve better error detection and correction. The study of the factorization of $x^n - 1$ in these rings formed the basis of encoding and decoding operations. Relatively, it has been indicated through comparative studies that these codes covering Gaussian integers are better than the traditional codes over Galois rings in some noise profiles, particularly in burst error scenarios or low SNR channels. Their suitability to modular arithmetic also implies their suitability to secure and quantum-resistant communication protocols.

This work can be extended in a number of ways in the future:

- Minimization of decoding algorithms, especially in the case of long codes, in order to decrease the computational complexity–accuracy trade-off.
- Going to quaternion and even octonion integers to seek structural benefits in other algebraic settings.
- Understanding the performance of these codes in post-quantum communicational systems, as well as blockchain consensus mechanisms and safe distributed systems.

Finally, alternant codes over Gaussian integers constitute an interesting family of algebraically robust but practically relevant error-correcting codes. Ongoing efforts in this direction could bring about new generations of codes that satisfy the requirements of more complex and security-sensitive communication infrastructures.

**Author Contributions:** M.S.: conceptualization; methodology; software; formal analysis; investigation; writing—original draft; writing—review & editing; project administration. N.A.A.: conceptualization; validation; writing—review & editing; project administration. All authors have read and agreed to the published version of the manuscript.

**Funding:** The researchers would like to thank the Deanship of Graduate Studies and Scientific Research at Qassim University for their financial support (QU-APC-2025).

**Data Availability Statement:** The original contributions presented in this study are included in the article.

**Acknowledgments:** We are also deeply grateful to our beloved mentor and true gentleman, Tariq Shah, whose vision and guidance have profoundly inspired our journey as researchers.

**Conflicts of Interest:** The authors declare no conflicts of interest.

## References

1. Dresden, G.; Dymàček, W.M. Finding factors of factor rings over the Gaussian integers. *Am. Math. Mon.* **2005**, *112*, 602–611. [CrossRef]

2. Freudenberger, J.; Ghaboussi, F.; Shavgulidze, S. New coding techniques for codes over Gaussian integers. *IEEE Trans. Commun.* **2013**, *61*, 3114–3124. [CrossRef]
3. Sajjad, M.; Shah, T.; Xin, Q.; Almutairi, B. Eisenstein field BCH codes construction and decoding. *AIMS Math.* **2023**, *8*, 29453–29473. [CrossRef]
4. De Andrade, A.A.; Palazzo, R., Jr. Construction and decoding of BCH codes over finite commutative rings. *Linear Algebra Its Appl.* **1999**, *286*, 69–85. [CrossRef]
5. Sajjad, M.; Shah, T.; ul Haq, T.; Almutairi, B.; Xin, Q. SPN based RGB image encryption over Gaussian integers. *Heliyon* **2024**, *10*, e30353. [CrossRef]
6. Sajjad, M.; Shah, T.; Alammari, M.; Alsaud, H. Construction and decoding of BCH-codes over the Gaussian field. *IEEE Access* **2023**, *11*, 71972–71980. [CrossRef]
7. Sajjad, M.; Shah, T.; Serna, R.J. Designing Pair of Nonlinear Components of a Block Cipher over Gaussian Integers. *Comput. Mater. Contin.* **2023**, *75*, 5287–5305. [CrossRef]
8. Byrne, E.; Fitzpatrick, P. Gröbner bases over Galois rings with an application to decoding alternant codes. *J. Symb. Comput.* **2001**, *31*, 565–584. [CrossRef]
9. De Andrade, A.A.; Shah, T.; Khan, A. A note on linear codes over semigroup rings. *Trends Comput. Appl. Math.* **2011**, *12*, 79–89. [CrossRef]
10. Shah, T. A note on ascend and descend of factorization properties. *Bull. Korean Math. Soc.* **2006**, *43*, 419–424. [CrossRef]
11. Shah, T. Relative ascent and descent in a domain extension. *Int. Electron. J. Algebra* **2010**, *7*, 34–46.
12. Shah, T.; Medhat, S. Stability of some integral domains on a pullback. *Mat. Vesn.* **2012**, *64*, 109–123.
13. Xie, C.; Chen, H.; Li, C.; Mesnager, S. Constructions of self-orthogonal linear codes and dual-containing BCH codes. *IEEE Trans. Inf. Theory* **2025**, *71*, 5049–5062. [CrossRef]
14. Galindo, C.; Hernando, F.; Martín-Cruz, H. New quantum codes from homothetic-BCH codes. *arXiv* **2025**, arXiv:2503.13069.
15. Lemoine, A.; Mora, R.; Tillich, J.P. Understanding the new distinguisher of alternant codes at degree 2. *Des. Codes Cryptogr.* **2025**, 1–23. [CrossRef]
16. Tang, N.; Han, Y.S.; Pei, D.; Chen, C. A Fast Decoding Algorithm for Generalized Reed-Solomon Codes and Alternant Codes. *arXiv* **2025**, arXiv:2502.02356.
17. Norton, G.H.; Sălăgean, A. On Efficient Decoding of Alternant Codes over a Commutative Ring. In Proceedings of the Cryptography and Coding: 7th IMA International Conference, Cirencester, UK, 20–22 December 1999; Springer: Berlin/Heidelberg, Germany; pp. 173–178.
18. Byrne, E.; Fitzpatrick, P. Hamming metric decoding of alternant codes over Galois rings. *IEEE Trans. Inf. Theory* **2002**, *48*, 683–694. [CrossRef]
19. Sajjad, M.; Shah, T.; Abbas, M.; Alammari, M.; Serna, R.J. The impact of alternant codes over Eisenstein integers on modern technology. *Comput. Appl. Math.* **2025**, *44*, 95. [CrossRef]
20. Zhang, K.; Dai, J.; Yu, X.; Zhang, G. Distance correction range-free localization algorithm for WSNs. *Ain Shams Eng. J.* **2024**, *15*, 102924. [CrossRef]
21. Molelekeng, B. Arithmetic in the Ring of Gaussian Integers. Ph.D. Thesis, University of the Witwatersrand Johannesburg, Johannesburg, South Africa, 2022.
22. Abu-Osba, E.A. Von Neumann inverses and cryptography. *Dirasat Pure Sci.* **2009**, *36*, 1–4.
23. Abu-Osba, E.A.; Henriksen, M.; Alkam, O.; Smith, F.A. The maximal regular ideal of some commutative rings. *Comment. Math. Univ. Carol.* **2006**, *47*, 1–10.